

ENGLISH TRANSLATION OF ANNEXES
TO THE IPER

ES1904(Amended)

10/549892

JC17 Rec'd PCT/PTO 16 SEP 2005

Claims:

- 1 1. (amended) A method of preventing virus infection by detecting
2 the virus infection in a network, comprising steps of:
3 obtaining communication information when a virus
4 intrudes;
5 detecting a virus source computer based on the
6 communication information obtained;
7 sending a message announcing an antivirus attack on the
8 virus source computer; and
9 making the antivirus attack on the virus source computer.
- 1 2. (amended) A method of preventing virus infection according to
2 Claim 1, wherein:
3 a decoy accessible through the network is provided to a
4 computer that monitors intrusion of a virus, for receiving access
5 to said decoy to obtain communication information and to detect
6 virus intrusion; and
7 said decoy is one or more of a decoy folder stored in a
8 storage unit, a decoy application stored in the storage unit, and a
9 server formed virtually in the storage unit.
- 1 3. A method of preventing virus infection according to Claim
2 1, wherein:
3 said attack is made by imposing a high load on the virus
4 source computer.
- 1 4. A method of preventing virus infection according to Claim

2 3, wherein:

3 said high load is imposed on the virus source computer by
4 increasing traffic of said computer.

1 5. A method of preventing virus infection according to Claim
2 3, wherein:

3 said high load is imposed on the virus source computer by
4 sending a large number of requests to which a CPU of said
5 computer should respond.

1 6. (amended) A system for preventing virus infection by detecting
2 the virus infection in a network, comprising:

3 a communication information analysis means that detects
4 intrusion of a virus, and then on detecting virus intrusion, detects
5 a virus source computer based on communication information
6 obtained when the virus intrudes;

7 a computer attack means that makes an antivirus attack
8 on the virus source computer through the network, for
9 suppressing operation of the virus; and

10 a message sending means that sends a message for
11 announcing a start of the attack, to the infected computer.

1 7. (amended) A system for preventing virus infection according to
2 Claim 6, wherein:

3 said system further comprises a decoy means accessible
4 through the network; and

5 said communication information analysis means detects
6 virus intrusion into said decoy means, and on detection of the

7 virus intrusion, detects a virus source computer, based on the
8 communication information obtained when the virus intrudes.

1 8. A system for preventing virus infection according to Claim
2 6, wherein:

3 said computer attack means imposes a high load on the
4 virus source computer.

1 9. (amended) A system for preventing virus infection according to
2 Claim 8, wherein:

3 said computer attack means imposes the high load on the
4 virus source computer by increasing traffic of said computer.

1 10. A system for preventing virus infection according to Claim
2 8, wherein:

3 said computer attack means imposes the high load on the
4 virus source computer by sending a large number of requests to
5 which a CPU of said computer should respond.

1 11. (amended) A system for preventing virus infection according to
2 one of Claims 6, 7, 8, 9 and 10, wherein:

3 said system further comprises a detection report
4 transmission means that sends a detection report to an
5 administrator of the virus source computer; and

6 said computer attack means continues to make the
7 antivirus attack on the virus source computer until a
8 countermeasure against the virus has been completed.

1 12. A system for preventing virus infection according to Claim
2 6, wherein:

3 said decoy means is a decoy folder realized by an
4 application provided in a decoy server that is formed virtually in
5 a storage unit of a computer connected to the network.

1 13. A system for preventing virus infection according to Claim
2 6, wherein:

3 said decoy means is a decoy application realized as an
4 application provided in a decoy server that is formed virtually in
5 a storage unit of a computer connected to the network.

1 14. (deleted)

1 15. (amended) A system for preventing virus infection according to
2 one of Claims 6, 7, 8, 9 and 10, further comprising:

3 an alarm sound generation means that generates an alarm
4 sound in a attacking terminal unit at a start of the attack or after
5 the start of the attack.

1 16. (amended) A system for preventing virus infection according to
2 one of Claims 6, 7, 8, 9 and 10, further comprising:

3 a requesting means that notifies a network address of the
4 virus source computer to another computer connected to the
5 network and requests to said computer for making an antivirus
6 attack on the virus source computer.

1 17. A system for preventing virus infection by detecting the

2 virus infection in a network, comprising:

3 a request receiving means that receives a request for
4 making an antivirus attack on a virus source computer; and

5 a computer attack means that makes an antivirus attack
6 on said virus source computer through the network for
7 suppressing operation of a virus, based on said request received.

1 18. (amended) A program for making a computer prevent virus
2 infection, wherein:

3 said program makes said computer realize:

4 a communication information analysis means that detects
5 intrusion of a virus, and then on detecting virus intrusion, detects
6 a virus source computer based on communication information
7 obtained when the virus intrudes;

8 a computer attack means that makes an antivirus attack
9 on the virus source computer through the network, for
10 suppressing operation of the virus; and

11 a message sending means that sends a message for
12 announcing a start of the attack, to the infected computer.

1 19. (deleted)

1 20. (added) A system for preventing virus infection by detecting
2 the virus infection in a network, comprising:

3 a communication information analysis means that detects
4 intrusion of a virus, and on detecting virus intrusion, detects a
5 virus source computer, based on communication information
6 obtained when the virus intrudes;

7 a computer attack means that makes an antivirus attack
8 on the virus source computer through the network, for
9 suppressing operation of the virus; and

10 an alarm sound generation means that generates an alarm
11 sound in an attacking terminal unit at a start of the attack or
12 after the start of the attack.

1 21. (added) A system for preventing virus infection by detecting
2 the virus infection in a network, comprising:

3 a communication information analysis means that detects
4 intrusion of a virus, and on detecting virus intrusion, detects a
5 virus source computer, based on communication information
6 obtained when the virus intrudes;

7 a detection report transmission means that sends a
8 detection report to an administrator of the virus source computer.